ATTORNEY DOCKET NO. LOGIN-RENEWAL/SCH
Serial No.: 09/681,570

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Scott C. Harris	Group Art Unit 2137
Appl. No.	:	09/681,570	
Filed	:	May 1, 2001	
For	:	LOGIN RENEWAL BASED ON DEVICE SURROUNDINGS	
Examiner	:	T. M. Norris	

Applicants brief on appeal

United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant herewith files this brief on appeal, thereby perfecting the notice of appeal originally filed on September 16, 2005. Note that the due date for response of this notice of appeal is actually November 17, 2005, as stated in for the Notice of Panel Decision that was mailed on October 17, 2005. Please charge the appeal brief fee to deposit account 50-1387 (small entity).

CERTIFICATE OF FAX TRANSMISSION

I hereby certify that this correspondence and all marked attachments are being facsimile transmitted to the Patent and Trademark Office on the date shown below:

11-17-05
Date of Deposit

Scott Harris
Signature

Scott Harris
Typed or Printed Name of Person

The sections required by section 41.37 follow:

Real party in interest.

The inventor, Scott C. Harris, is the real party in interest.

Related appeals and interferences

There are no known related appeals and/or interferences.

Status of claims

Claims 1 through 21 are pending in the application, and claims 1, 3-4, 6 and 8-14 are rejected. Claims 7 and 18 were indicated as allowable. Claims 2, and 15-21 are apparently withdrawn from consideration.

Status of amendments

No amendment was filed subsequent to the final rejection

Summary of claimed subject matter

Claim 1 requires a computer peripheral that detects information about a surrounding of the computer. As described in paragraph 10, this can be any of the sensory devices within the PDA.

A computer runs a routine that allows the user to identify themselves to the computer. For example, a security prompt at 200 is described paragraph 8, and in figure 2.

Claim 1 further requires that the computer determines a first surrounding at a time of the user identification, maintains the computer unlocked while within the first surrounding and causes the computer to lock when the computer has moved from the first surrounding by a predetermined and relative amount. This is described in paragraph 10, where 220 describes a periodic check to detect new surroundings which may include a new position. Paragraph 11 describes that the computer is only locked when the user moves more than a certain amount.

Claim 8 defines a first security operation which allows a computer to obtain access to resources of a computer, which is described in paragraph 9. Claim 8 further defines determining surrounding information both at a first time and a second time, see generally paragraphs 10 and 11. Claim 8 further defines allowing continued access to the resources only so long as the second surrounding does not differ from the first surroundings by more than a specified relative amount of distance. See paragraphs 10 and 11.

Grounds of rejection to be reviewed on appeal

-Are claims 1, 3, 6, 9 and 13 properly rejected under 35 USC 103 as being unpatentable over Murphy '500 in view of Guthrie?

-Are claims 4-5, 10 and 12 properly rejected over Murphy in view of Guthrie in view of Murphy '082?

-Are claims 8, 11 and 14 properly rejected over Murphy in view of Guthrie and further in view of Jones?

Argument

Rejections under section 103

The rejection of claims 1, 3, 6, 9 and 13 based on Murphy in view of Guthrie is respectfully traversed.

Claim 1 defines a computer peripheral that detects information about a first surrounding, a computer that runs a routine "which allows a user to identify themselves to the computer and controls access to the computer based on said identify", and where the computer determines the first surrounding at a time of identification, maintains the computer unlocked while the computer is within the first surrounding, and causes the computer to lock when the computer is detected to have moved from the first surrounding by a predetermined and relative amount. Note an important feature of claim 1, overlooked by the Patent Office's current rejection, is that the computer must be detected to have moved from "the first surrounding", that is, the surrounding that the computer "determines at the time of identification". Claim 1 defines that a user "identify themselves to the computer", and "controls access ... based on said identify and said first surrounding". Claim 1 also defines that the computer is caused to "lock when the computer is detected to have moved from said first surrounding by a predetermined and relative amount" (emphasis added).

Considering the scope and content of the Murphy prior art, shows that Murphy teaches a decryption chip. That decryption chip is licensed only for use in a specified market. The decryption chip can only be used in that specified market. That specified market has nothing to do with "the first surrounding", that is, the surrounding that the computer "determines at the time of identification". The market is the market, and the market has nothing to do with the surrounding at the time of identification. The chip has a built-in positioning system. When the chip is moved outside the market area, the positioning system detects that, and the chip is disabled. Again, this has nothing to do with any kind of position that is detected at 'the time of identification".

Moreover, Murphy teaches nothing about login, and has no teaching that could reasonably be applied to a login. All of Murphy's teaching is about using the chip only within a licensed or specific market. Further, Murphy teaches nothing about the claim limitation of determining "a first surrounding at a time of user identification". In fact, this feature seems foreign to the whole notion of a region-specific chip. Murphy would never need to detect this "first surrounding". Murphy only needs to determine if it is in the region, or out of the region, at any time. The "region", that is, where the chip physically is at some hypothetical time of any user identification, would be plainly irrelevant, even if Murphy did so disclose.

Murphy also teaches nothing about relative distance. The rejection attempts to glean this from column 8, lines 1 through 6 of Murphy, which describes how the receiver/processor 203I has the location coordinates x,y,z of the licensed site and coordinates of a region that is centered at that location. Column 8 describes that the diameter may vary with the location of the site and the circumstances. However, even if the diameter of the region may vary, this suggests nothing about causing the computer to lock when the computer is detected to have moved from the "first surrounding" by a predetermined and relative amount. In fact, column 8 appears to teach away from the "predetermined amount", since it states that the diameter may vary with the circumstances. If the diameter varies, it is not "determined", rather it is variable.

Either way, the location is ALWAYS the location of the licensed site. There is never any teaching or suggestion of determining the first surrounding at the time of user identification as claimed. Murphy is quite simply devoid of this kind of teaching.

Guthrie teaches a basic login system. The rejection incorrectly reasons that the region locking of Murphy could be used with a login system of Guthrie.

It is entirely hindsight to combine a region specific decryption chip such as Murphy, with a login system such as Guthrie. The mere combination between the two is based on hindsight and based on the teaching of the present application, not based on the contents of the prior art. Therefore, with all due respect, this is an improper combination.

Even if combined, the hypothetical combination still teaches nothing about causing the computer to lock when movement by a predetermined and relative amount, relative to the "first surrounding" is detected. Moreover, note that all teaching in Murphy is about the location coordinates of the licensed site, see for example column 8, lines 13-14. There is no teaching or suggestion of a "first surrounding", determined "at a time of user identification", much less using that first surrounding for any purpose.

Even if Murphy and Guthrie were combined, the hypothetical combination still would not teach or suggest a computer that "determines a first surrounding at a time of user identification". The hypothetical combination would be a Murphy type system in which licensed site coordinates were maintained, along with a login system such as shown in Guthrie.

Claim 1 should therefore be allowable for these reasons.

Claim 4 defines that the surrounding includes a view that is seen by the computer. Claim 4 was rejected over Murphy in view of Guthrie and further in view of Murphy '082. Murphy '082 teaches a system which uses image authentication information, that allows authenticating a digital image. Nowhere is there any teaching or suggestion of using this for anything associated with login. More specifically, however, nothing in 082 teaches using an image to determine a first surrounding for controlling access to a computer, and using second image at a second time to determine if the system has moved by more than a specified amount.

Claim 5, which specifically defines an image of a user, should be allowable for similar reasons. Murphy 082 teaches authentication information in a digital image, but teaches nothing about comparing an image obtained at one time with another image obtained at a different time. Moreover, this is inconsistent with Murphy's teaching of an x,y,z coordinate of a licensed market for the chip.

Claim 8 is rejected based on Murphy in view of Guthrie and further in view of Jones. With all due respect, Murphy in view of Guthrie would not be operatively combined by one having ordinary skill in the art for reasons discussed above. If combined, as described above, the hypothetical combination still would not teach or suggest determining first surrounding information associated with the first security operation and second surrounding information at times subsequent to the time when the first surrounding was obtained. Hence, this claim should be allowable for analogous reasons to those discussed above.

Jones defines obtaining additional security information before allowing access to resources. However, this reference is cited while entirely ignoring the context of the claim. Claim 8 requires allowing the continued access "only so long as the second surroundings information does not differ from said first surroundings information by more than a specified relative amount of distance". If it so differs, the new security operation is required to obtain the access. While Jones does teach using a new security operation in certain circumstances, it does not teach that those circumstances relate to differences between the surroundings information as claimed.

Claim 8 should therefore be allowable. The dependent claims should be allowable for analogous reasons to the above.

In summary, and with all due respect, the rejection by the Patent Office has misapprehended the contents of the prior art relative to the claims, and with all due respect, the rejection by the Patent Office should be reversed.

Appl. No. : 09/681,570
Filed : May 1, 2001

Claims Appendix

1. A system comprising:

a computer peripheral, detecting information about a first surrounding of the computer;

a computer, running a routine which allows a user to identify themselves to the computer, and controls access to the computer based on said identify and said first surrounding; and

wherein said computer determines a first surrounding at a time of user identification, and maintains the computer unlocked while the computer is within said first surrounding, and causes the computer to lock when the computer is detected to have moved from said first surrounding by a predetermined and relative amount.

3. A system as in claim 1, wherein said surrounding is a physical location of the computer, as detected by an automatic position location device.

4. A system as in claim 1, wherein said surrounding includes a view that is seen by the computer.

5. A system as in claim 4, wherein said view includes an image of a user.

6. A system as in claim 2, further comprising a failure processing routine, which processes failures in login by increasing security for each of a plurality of times when a login fails.

7. A system comprising:

a computer peripheral, detecting information about a current surrounding of the computer;

a computer, running a routine which allows a user to identify themselves to the computer, and controls access to the computer based on said identify and said current surrounding;

wherein said computer determines a first surrounding at a time of user identification, and maintains the computer unlocked while the computer is in said first surrounding, and causes the computer to lock when the computer is detected to vary from said first surrounding by a predetermined amount; and

increasing a security of the computer when a user powers down the computer in response to being prompted to identify themselves.

8. A method, comprising:

carrying out a first security operation which allows a user to obtain access to resources of the computer;

determining surroundings information, including first surroundings information associated with said first security operation, and second surroundings information at times subsequent to said first surroundings information; and allowing continued access to resources of the computer only so long as said second surroundings information does not differ from said first surroundings information by more than a specified relative amount of distance ~~threshold~~, and if said second surroundings information differs from said first surroundings information by more than said specified threshold, then requiring a new security operation to obtain said access to said resources.

9. A method as in claim 8, wherein said surroundings information is information indicative of a physical location of the computer, and said determining comprises using an automatic position determining device to determine said position.

10. A method as in claim 8, wherein said surroundings information is information indicative of an image of a proximity of said computer, and said determining comprises using a camera to determine said image.

11. A method as in claim 9, further comprising determining a difference between said first and second surroundings information, determining a distance between the physical locations indicated by said first and second surroundings information, determining if said distance is greater than a predetermined threshold, and allowing said continued access only when said distance is not greater than said predetermined threshold.

12. A method as in claim 10, further comprising determining a difference between a first image representing said first surroundings information, and a second image representing said second surroundings information, using automated machine vision techniques.

13. A method as in claim 8, wherein said first security operation comprises determining whether a user has successfully responded to a request for user-security information, and for each of the plurality of times that the user does not successfully respond to said request for user-security information, increasing an aspect of security.

14. A method as in claim 13, wherein said increased aspect of security includes entry of secret personal information.

16. A method, comprising:

detecting an attempt to obtain access to computer resources and maintaining a number of times that said attempt has been made;

for each of said plurality of attempts, increasing a security of said computer resources by encrypting specified files, wherein additional files are encrypted each time that an attempt to obtain access is made.

18. A method, comprising:

carrying out a first security operation which allows a user to obtain access to resources of the computer;

determining surroundings information, including first surroundings information associated with said first security operation, and second surroundings information at times subsequent to said first surroundings information;

allowing continued access to resources of the computer only so long as said second surroundings information does not differ from said first surroundings information by more than a specified threshold, and if said second surroundings information differs from said first surroundings information by more than said specified threshold, then requiring a new security operation to obtain said access to said resources; and

wherein said determining comprises triangulating to determine a position.

19. A system comprising:

a computer, running a routine which allows a user to identify themselves to the computer, and

a file access detecting part, detecting access to a specified higher security file on said computer, and requiring a user to re-identify themselves to the computer upon said detecting said access to said specified higher security file, but not requiring the user to re identify themselves to the computer upon detecting access to files other then said specified higher security files.

20. A system as in claim 19, wherein said higher security files are manually marked as high security files.

21. A system as in claim 19, wherein said file access detecting part automatically detects specified words in said files, and automatically determines files including said specified words as being said higher security files.

Appl. No.	**:**	**09/681,570**
Filed	**:**	**May 1, 2001**

Evidence Appendix: None

Related Proceedings Appendix: None

Appl. No. : 09/681,570
Filed : May 1, 2001

Please charge any fees due in connection with this response to Deposit Account No. 50-1387.

Respectfully submitted,

Date: 11-17-05

Scott C. Harris
Reg. No. 32,030

Customer No. 23844
Scott C. Harris, Esq.
P.O. Box 927649
San Diego, CA 92192
Telephone: (619) 823-7778
Facsimile: (858) 678-5082